UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

ENAYATULLAH KHWAJA,
also known as "Nat,"
ABDULRAHMAN KHWAJA,
RANA RAHIMI,
SHIKEBA RHAMATZADA,
ROBERTO SAENZ,
MAYNOR MELENDEZ-MENDOZA,
and NASEEM BOKHARI,
also known as "Sammy,"

Defendants.

18 Cr. 607 (JMA)

MEMORANDUM OF LAW IN SUPPORT OF ABDULRAHMAN KHAWAJA AND SHIKEBA RHAMATZADA'S JOINT OMNIBUS PRETRIAL MOTION

Roland G. Riopelle
SERCARZ & RIOPELLE, LLP
810 Seventh Ave., Suite 620
New York, NY 10019

Attorneys for Abdulrahman Khwaja

Michael Tremonte
Noam Biale
SHER TREMONTE LLP
90 Broad St., 23rd Floor
New York, NY 10004

Attorneys for Shikeba Rhamatzada

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

PRELIMINARY STATEMENT 1

FACTUAL BACKGROUND 2

I. The National Companies 2

II. The Indictment 2

III. The Investigation and Pretrial Proceedings 4

A. Wiretaps of Defendants and the Szwalek Affidavit 4

B. Searches and Seizures at the Defendants' Homes and Offices 6

ARGUMENT 8

I. Counts One, Five, and Six of the Indictment Should Be Dismissed as Duplicitous or Severed 8

A. Count One Alleges Multiple Conspiracies Under the Guise of One 10

B. The Duplicity Inherent in Count One Infects the Other Counts That Lump Abdul and Shikeba Together with the Tronix Defendants 14

II. The Court Should Sever the Trials of the National Defendants and the Tronix Defendants 16

A. The Defendants Are Misjoined Under Rule 8 16

B. Joinder with the Tronix Defendants Is Unfairly Prejudicial to the National Defendants 17

III. The Court Should Suppress the Fruits of the Searches of National's Office and Abdul and Shikeba's Homes 21

A. The Warrants Here Violated Fourth Amendment Requirements 22

1. The Particularity Requirement and Prohibition Against Overbreadth 22

2. The Warrants Are Facially Invalid Because They Authorize the Seizure of an Unrestricted Range of Documents and Devices without Limitation 23

3. The Warrant Application Failed to Satisfy the Probable Cause Standard as to Shikeba and Abdul's Homes 27

4. The Search of Shikeba's Home Violated Rule 41 29

5. The Government Failed to Search the Seized Electronic Devices Promptly and Its Ultimate Search of the Devices Was an Unguided Fishing Expedition 30

i. Failure to Search Electronic Devices 31

ii. Absence of Search Protocol 33

IV. The Court Should Suppress the Fruits of the Wiretap Or, in the Alternative, Order a *Franks* Hearing 36

A. A Wiretap Should Only Be Authorized Based on a Full and Complete Showing of Probable Cause and Necessity, and Agents Conducting a Wiretap Must Take Care to Ensure the Privacy of Its Targets 36

B. The Wiretap Application Failed to Establish the Necessity of a Wiretap as to Abdul and Shikeba 39

C. The Szwalek Affidavit's Claims of Probable Cause and Necessity Were Based on Material Omissions 41

D. The Government Failed in Its Minimization Duty 43

V. The Court Should Order a Bill of Particulars as to the Structuring Count and As to the Travel and Transportation in Aid of Racketeering Count 44

VI. The Court Should Order the Government to Produce its File Concerning the Internal Revenue Service's Audit of the National Companies Form 8300 Compliance 47

VII. The Court Should Order That a Jury Questionnaire Be Used During Voir Dire 47

CONCLUSION 50

TABLE OF AUTHORITIES

Page(s)

Cases

Berger v. New York,
388 U.S. 41 (1967) 36, 41

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 22, 34

Dalia v. United States,
441 U.S. 238 (1979) 37, 41

Franks v. Delaware,
438 U.S. 154 (1978) 36, 38

Gelbard v. United States,
408 U.S. 41 (1972) 36

Groh v. Ramirez,
540 U.S. 551 (2004) 23

Illinois v. Gates,
462 U.S. 213 (1983) 29

In re 650 Fifth Ave. & Related Properties,
830 F.3d 66 (2d Cir. 2016) 23, 26

Kotteakos v. United States,
328 U.S. 750 (1946) 15

Matter of the Search of Apple iPhone, IMEI 013888003738427,
31 F. Supp. 3d 159 (D.D.C. 2014) 35

Rosales-Lopez v. United States,
451 U.S. 182 (1981) 47

Scott v. United States,
436 U.S. 128 (1978) 37, 43

Silverman v. United States,
365 U.S. 505 (1961) 29

Steagald v. United States,
451 U.S. 204 (1981) 29

United States v. Attanasio,
870 F.2d 809 (2d Cir. 1989)..... 9, 16

United States v. Bianco,
998 F.2d 1112 (2d Cir. 1993)..... 38

United States v. Blackmon,
273 F.3d 1204 (9th Cir. 2001) 37

United States v. Bortnovsky,
820 F.2d 572 (2d Cir. 1987)..... 45

United States v. Bowline,
593 F.2d 944 (10th Cir. 1979) 13

United States v. Brandon,
17 F.3d 409 (1st Cir. 1994) 13

United States v. Branker,
395 F.2d 881 (2d Cir. 1968)..... 18, 19

United States v. Burke,
517 F.2d 377 (2d Cir. 1975)..... 30

United States v. Canfield,
212 F.3d 713 (2d Cir. 2000)..... 38

United States v. Capra,
501 F.2d 267 (2d Cir. 1974)..... 38

United States v. Cervone,
907 U.S. 332 (2d Cir. 1990)..... 9, 16

United States v. Clark,
638 F.3d 89 (2d Cir. 2011)..... 26, 29

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 34

United States v. Concepcion,
579 F.3d 214 (2d Cir. 2009)..... 37, 41

United States v. Costin,
No. 5 Cr. 38, 2006 WL 2522377 (D. Conn. July 31, 2006)..... 23

United States v. Dale,
991 F.2d 819 (D.C. Cir. 1993) 24

United States v. Debbi,
244 F. Supp. 235 (S.D.N.Y. 2003) 31, 32, 33

United States v. Debbi,
No. 02 CR. 808(JSR), 2003 WL 1922928 (S.D.N.Y. Mar. 31, 2003) 32

United States v. Dioguardi,
332 F. Supp. 7 (S.D.N.Y. 1971) 11

United States v. Eppolito,
543 F.3d 25 (2d Cir. 2008) 11

United States v. Feyrer,
333 F.3d 110 (2d Cir. 2003) 9

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013) 22, 25, 34

United States v. Geaney,
417 F.2d 1116 (2d Cir. 1969) 14

United States v. Gigante,
538 F.2d 502 (2d Cir. 1976) 37

United States v. Gilbert,
504 F. Supp. 565 (S.D.N.Y. 1980) 18, 19, 20

United States v. Giordano,
416 U.S. 505 (1974) 37, 38, 39

United States v. Goffer,
756 F. Supp. 2d 588 (S.D.N.Y. 2011) 38, 43, 44

United States v. Gonzalez,
No. 86 CRIM. 1057 (WCC), 1987 WL 6923 (S.D.N.Y. Feb. 6, 1987) 27

United States v. Goodman,
285 F.2d 378 (5th Cir. 1960) 16

United States v. Griffith,
867 F.3d 1265 (D.C. Cir. 2017) 24, 29

United States v. Halper,
590 F.2d 422 (2d Cir. 1978) 9, 15

United States v. Hood,
210 F.3d 660 (6th Cir. 2000) 16

United States v. Jacobson,
4 F. Supp. 3d 515 (E.D.N.Y. 2014) 22

United States v. Kelly,
349 F.2d 720 (2d Cir. 1965) 18

United States v. King,
991 F. Supp. 77 (E.D.N.Y. 1998) 44

United States v. Kow,
58 F.3d 423 (9th Cir. 1995) 24

United States v. Lambus,
897 F.3d 368 (2d Cir. 2018) 39

United States v. Leon,
468 U.S. 897 (1984) 39

United States v. Lilla,
699 F.2d 99 (2d Cir. 1983) 37

United States v. Lumiere,
No. 16 Cr. 483, 2016 WL 7188149 (S.D.N.Y. Nov. 29, 2016) 33

United States v. MacPherson,
424 F.3d 183 (2d Cir. 2005) 45

United States v. Maldonado–Rivera,
922 F.2d 934 (2d Cir. 1990) 11

United States v. Marcus Schloss & Co.,
710 F. Supp. 944 (S.D.N.Y. 1989) 13

United States v. Marcus,
628 F.3d 36 (2d Cir. 2010) 12

United States v. Marlinga,
No. CRIM 04-80372, 2005 WL 513494 (E.D. Mich. Feb. 28, 2005) 13

United States v. McCabe,
No. 05-CR-0237(S-1)(DRH), 2006 WL 2990480 (E.D.N.Y. Oct. 19, 2006)..... 17

United States v. McDermott,
245 F.3d 133 (2d Cir. 2001)..... 11

United States v. Metter,
860 F. Supp. 2d 205 (E.D.N.Y. 2012) 31, 33

United States v. Munoz-Franco,
986 F. Supp. 70 (D.P.R. 1997)..... 13, 16

United States v. Orena,
883 F. Supp. 849 (E.D.N.Y. 1995) 44

United States v. Quinones,
511 F.3d 289 (2d Cir. 2007)..... 48

United States v. Rajaratnam,
719 F.3d 139 (2d Cir. 2013)..... 38, 43

United States v. Rajaratnam,
No. 09 CR 1184 RJH, 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010) 38, 42

United States v. Ramirez-Martinez,
273 F.3d 903 (9th Cir. 2001) 16

United States v. Rice,
478 F.3d 704 (6th Cir. 2007) 39

United States v. Rigas,
281 F. Supp. 2d 660 (S.D.N.Y. 2003)..... 10

United States v. Riley,
906 F.2d 841 (2d Cir. 1990)..... 22

United States v. Rosenblatt,
554 F.2d 36 (2d Cir. 1977)..... 11

United States v. Salameh,
152 F.3d 88 (2d Cir. 1998)..... 47

United States v. Shellef,
502 F.3d 82 (2d Cir. 2007)..... 9

United States v. Shi Yan Liu,
239 F.3d 138 (2d Cir. 2000)..... 22

United States v. Shkreli,
260 F. Supp. 3d 247 (E.D.N.Y. 2017) 20, 21

United States v. Spinelli,
352 F.3d 48 (2d Cir. 2003)..... 18, 20

United States v. Sturdivant,
244 F.3d 71 (2d Cir. 2001)..... 8

United States v. Taylor,
816 F.3d 12 (2d Cir. 2016)..... 45

United States v. Torres,
901 F.2d 205 (2d Cir. 1990)..... 12, 45

United States v. Tureff,
853 F.2d 1037 (2d Cir. 1988)..... 8, 9, 16

United States v. Ulbricht,
858 F.3d 71 (2d Cir. 2017)..... 22, 26, 34

United States v. Vanwort,
887 F.2d 375 (2d Cir. 1989)..... 11, 12

United States v. Vilar,
No. S305CR621KMK, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007)..... 23, 24, 25

United States v. Viserto,
596 F.2d 531 (2d Cir. 1979)..... 13

United States v. Walser,
275 F.3d 981 (10th Cir. 2001) 35

United States v. Wey,
256 F. Supp. 3d 355 (S.D.N.Y. 2017)..... 23, 25, 26, 34

United States v. Zemlyansky,
945 F. Supp. 2d 438 (S.D.N.Y. 2013)..... 22, 23, 25, 38

Walczyk v. Rio,
496 F.3d 139 (2d Cir. 2007)..... 38

Zafiro v. United States,
506 U.S. 534 (1993) 17, 18

Statutes

18 U.S.C. § 1952 15

18 U.S.C. §§ 2510–2520 36

18 U.S.C. § 2515 ..... 36, 38

18 U.S.C. § 2518 ..... 36, 37

Rules

Federal Rule of Criminal Procedure 7 45

Federal Rule of Criminal Procedure 8 ..... 8, 9

Federal Rule of Criminal Procedure 12 1

Federal Rule of Criminal Procedure 14 17

Federal Rule of Criminal Procedure 41 ..... 7, 30

Federal Rule of Evidence 104 14

Federal Rule of Evidence 801 14

Other Authorities

Pager, D., *Discrimination in Law-Wage Labor Market: A Field Experiment*,
Am. Sociological Rev., Oct. 1, 2009. 48

Hoffman, K., *Racial bias in pain assessment and treatment recommendations, and false beliefs about biological differences between blacks and whites*,
Proceedings of the National Academy of Sciences, Apr. 4, 2016 48

PRELIMINARY STATEMENT

Defendants Abdulrahman Khwaja ("Abdul") and Shikeba Rhamatzada ("Shikeba"), by their undersigned attorneys, respectfully submit this memorandum of law in support of their motion for pretrial relief pursuant to Federal Rule of Criminal Procedure 12.

The fundamental flaw infecting the charging instrument, search warrants, and wiretap application in this case is the government's erroneous conflation of the businesses affiliated with Abdul and Shikeba (the "National Companies") and those affiliated with their cousin Enayatullah "Nat" Khwaja (the "Tronix Companies"). The indictment does not specifically allege any connection or relationship between the two sets of companies other than a familial relationship of the principals. Thus, neither the indictment nor the discovery contains a single specific allegation or piece of evidence showing that the National Companies and the Tronix Companies ever coordinated with each other; ever agreed to conduct business with each other; ever transacted with each other; or, indeed, *ever communicated with each other*.

Nevertheless, the indictment impermissibly lumps together the National Companies and the Tronix Companies, charging them in a misjoined single conspiracy, even though there is no connection, no coordination, and no mutual benefit between them. The mere fact that these companies were owned by two cousins and employed members of the same extended family is an improper basis for a single conspiracy charge, a joint trial, and investigative methods that were not predicated on individual probable cause or necessity.

Accordingly, Abdul and Shikeba respectfully move for an order (1) dismissing Counts One, Five, and Six of the indictment as duplicitous; (2) severing their trial from that of certain co-defendants; (3) suppressing the fruits of the search of their homes and of the office of National Electronics, Inc.; and (4) suppressing the fruits of the wiretap as to them, or, in the

alternative, ordering a *Franks* hearing. In addition, Abdul and Shikeba respectfully request an order (5) directing the government to provide a bill of particulars as to the structured financial transactions and travel in aid of racketeering activity it intends to prove at trial; (6) ordering the government to produce certain *Brady* material previously demanded by Abdul; and (7) permitting the use of a jury questionnaire during voir dire at trial.

FACTUAL BACKGROUND

I. The National Companies

The National Companies are a well-established group of companies that employ nearly fifty people and have operated in the wholesale and retail electronics business for nearly forty years, with sales in televisions, camcorders, VCRs, and now (due to technological changes in the electronics industry), cellular phones. Declaration of Michael Tremonte (hereinafter "Tremonte Decl.") ¶ 4. The National Companies have always—and continue to—focus predominantly on the North American, and specifically U.S., markets. *Id.* While the Companies have exported cellphones to South America through its affiliate ISK Corporation, the South American market has never been the primary focus of the business, *see id.* ¶¶ 5, 30, and sales into that market have never been more than a relatively minor stream of revenue, *id.*, Ex. R.

II. The Indictment

On November 7, 2018, a Grand Jury sitting in this district returned an indictment against Abdul and Shikeba, and others. *See* Tremonte Decl. ¶ 6 & Ex. A (hereinafter, the "Indictment"). Specifically, the Indictment identified Abdul as the owner and manager of National Electronics, Inc. ("National") and related companies, including Ishan International, Inc., ISK Corporation ("ISK"), Taban Company, Solid Wireless, Inc. ("Solid"), and Solid Electronics, Inc. (collectively, the "National Companies"). Indictment ¶ 3. It identified Shikeba as the president

of Solid and ISK, and as working with Abdul to manage Solid and other companies in Farmingdale. *Id.* ¶ 5. It charged Roberto Saenz ("Saenz"), an employee of ISK, as being "a go-between for ISK and its South American client base." *Id.* ¶ 6. Abdul, Shikeba, and Saenz are hereinafter referred to collectively as the "National Defendants."

The Indictment separately identified Enayatullah Khwaja ("Nat") as being the owner and manager of Tronix Telecom Corp. ("Tronix") and Sysco International, LLC ("Sysco" and, collectively, the "Tronix Companies"). *Id.* ¶ 2. There is no allegation that the National and Tronix Companies are jointly owned, managed, or operated. The Indictment charged two employees of Tronix, Maynor Melendez Mendoza ("Melendez Mendoza") and Naseem Bokhari ("Bokhari"). *Id.* ¶ 7. Nat, Melendez Mendoza, and Bokhari are hereinafter collectively referred to as the "Tronix Defendants." Finally, the Indictment charged Rana Rahimi ("Rahimi"), the sister of Nat and a cousin of Abdul, and the bookkeeper for National, Tronix, and Sysco. *Id.* ¶ 4.

The Indictment names the National Defendants in only three of the six counts: the money laundering conspiracy, structuring, and Travel Act violations. The National Defendants are *not* named in the Form 8300 count, the Currency Transmitting Report count, or the unlicensed money transmitting count. Specifically, Count One of the Indictment alleges a conspiracy by all of the defendants—the National Defendants and the Tronix Defendants alike—to launder money from October 2013 to November 2018. *Id.* ¶ 15. The money laundering conspiracy charge includes no specific factual allegations, but simply lists boilerplate language alleging the laundering of proceeds of various crimes. *See id.* The Indictment also alleges structuring of financial transactions (Count Five), without identifying any particular structured transaction; and interstate and foreign travel in violation of the Travel Act for the purpose of distributing the proceeds of the preceding charges (Count Six), without identifying any particular

travel or distribution transaction. The Indictment's substantive charges allege that the Tronix Defendants operated an unlicensed money transmitting business (Count Two), caused various banks to fail to file Currency Transmitting Reports (Count Three), and caused the failure to file IRS Forms 8300 (Count Four). As noted, the National Defendants (*i.e.*, Abdul, Shikeba, and National employees) were not alleged to have violated any of these requirements and were not charged with these substantive offenses.

III. The Investigation and Pretrial Proceedings

A. Wiretaps of Defendants and the Szwalek Affidavit

Prior to obtaining the Indictment, the government sought to intercept the defendants' telephone calls by means of a judicially-authorized wiretap. Initially, on June 2, 2017, the government sought and obtained authorization to tap Nat's phones for a one-month period. *See* Tremonte Decl., Ex. B ¶ 13. The wiretap of Nat's phones (and other individuals not indicted in this case) was reauthorized twice — once on June 30, 2017 and again on July 31, 2017. *Id.* ¶¶ 14-15. The government did not name Shekiba or Abdul as subject individuals or seek to intercept their communications until the *fourth* iteration of the wiretap application, which was filed and approved on August 30, 2017. *Id.* at 91.

The affidavit filed in support of the wiretap application by Special Agent John Szwalek, Jr. (the "Szwalek Affidavit" or the "Affidavit") did not allege any connection between the Tronix Companies and the National Companies. It alleged that ISK had previously sent shipments of cellphones to a Paraguayan company called Crystal Esteno Importer and Exporter. The Affidavit alleged that a purported member of a South American money laundering organization that had business dealings with Nat had also used Crystal Esteno to ship cocaine to various countries, but it did not link these drug shipments to any transactions involving ISK. *See id.* ¶¶ 59-60. The

Szwalek Affidavit also described the border search of Shikeba's phone, which, it alleged, revealed Whatsapp text exchanges regarding cash payments that purportedly evidenced structuring and payments from third parties. *Id.* ¶¶ 61-66. The Szwalek Affidavit also described a U.S. Customs and Border Protection ("CBP") Regulatory Audit of ISK that was conducted in 2017, and excerpted Whatsapp communications between Shikeba and others regarding the presence of CBP auditors at the ISK office. *Id.* ¶¶ 67-76. The Szwalek Affidavit noted that, as part of the audit, government auditors spoke to ISK employees, including Saenz, and communicated with Shikeba via email. *Id.* ¶ 67 n.14. It stated that the audit "noted a potential risk of negligence or fraud for export compliance as part of [a] scheme to conduct potential TBML activities." *Id.*

What the Szwalek Affidavit failed to state, however, is that ISK had fully cooperated with the audit and that, other than a few controls that CBP advised the company it could improve, no concern about possible money laundering or illegal activity was ever communicated to the company. Tremonte Decl. ¶ 9. Finally, while the Szwalek Affidavit set forth the government's asserted basis for probable cause as to Shikeba and (to a lesser extent) as to Abdul,[1] it did not mention either in its explanation of the *necessity* of the wiretap, other than to note that agents had successfully conducted searches of Shikeba and Abdul's phone at the border. Tremonte Decl., Ex. B, at ¶ 111.

[1] The Szwalek Affidavit's only assertions as to Abdul were that he is the owner of ISK and Solid Wireless; the bald assertion that he had "been identified as directly involved in the movement of money and connected to the import and export of goods associated with" the alleged criminal violations; that Special Agent Szwalek "believes" that a single wire communication between Shikeba and Abdul on June 6, 2017 included a discussion of "ways to conceal invoicing schemes that the FARHAT MLO utilizes to launder funds" without quotation of any such discussion, or any explanation of the basis for such belief; and that a report by Saenz to Abdul of wire transfers received, but not yet applied to specific invoices, was somehow indicative of money laundering activity. Tremonte Decl., Ex. B, pp. 11, 12, 47 & 55.

B. Searches and Seizures at the Defendants' Homes and Offices

On November 15, 2018, the government arrested the defendants, seized bank accounts held in the name of the National and Tronix Companies, and executed search warrants at, *inter alia*, the office of National, located at 500 Smith Street in Farmingdale, New York, Shikeba's home in Farmingdale, and Abdul's home in Syosset, New York. The affidavit filed in support of the search warrant application made no effort to distinguish between the National Companies and the Tronix Companies; it simply ascribed actions on behalf of either as being attributable to the "Khwaja Companies." Tremonte Decl., Ex. D, at ¶ 18. Consequently, the warrant application did not differentiate the probable cause as between the two sets of companies and instead baldly asserted that both were part of the same money laundering conspiracy.

On November 13, 2018, a magistrate judge in this district authorized the search and seizure warrants. The warrants themselves did not attach the application or incorporate it by reference. Instead, they included "Attachment H," which described the "items to be searched and seized." *See, e.g.*, Tremonte Decl., Ex. E, at 5. Attachment H listed the subject offenses, and authorized the seizure of "[a]ny and all business books and records relating to" (i) any of the Subject Premises and (ii) the Subject Vehicle (there was none, and the reference to a "Subject Vehicle" appears to be carried over from search warrant in a prior, unrelated case); it also authorized the seizure of "[a]ny and all records" that were "in the names of" all of the defendants and others, as well as documents "including but not limited to" records of any investments in twelve companies. *Id.* ¶ 2, 5. Attachment H also authorized the search and seizure of any computer or electronic device. *Id.* ¶ 6. Neither Attachment H nor the warrants themselves contained a date limitation for the documents to be seized. *See generally id.* In other words, the warrants authorized the indiscriminate seizure of *all* computers and electronic devices

(without any subject matter restriction), *all* books and records related to any one of the numerous physical addresses to be searched—homes and offices alike—and *all* records in the name of or relating to numerous individuals and companies, for an indefinite period of time.

On November 15, 2018, law enforcement officials executed the warrants. During the search of Shikeba's home, the government seized items plainly unrelated to the charged crimes, including the passports, birth certificates, and social security cards of Shikeba's husband and children, Shikeba's marriage certificate, laptops and iPads belonging to Shikeba's children that they used for their schoolwork, and business records pertaining to Shikeba's husband's art gallery. *See* Tremonte Decl., Ex. H (Letter to Government, dated Dec. 10, 2018). The agents failed to provide Shikeba with a copy of the warrant and did not leave an inventory of the items they seized, in violation of the requirements of Federal Rule of Criminal Procedure 41. *Id.*

After the government seized dozens of electronic devices, and then produced in discovery their entire contents without any evidence of having conducted a responsiveness review, the defendants requested—and the Court ordered—the government to produce the search protocol it had used to search the devices. Tremonte Decl. ¶¶ 17-18. By letter dated June 14, 2019, Dkt. # 166, the government acknowledged that it had not actually begun searching the devices. Tremonte Decl., Ex. J, at 2 ("After the use of [software programs to extract data from the devices], the government will have a better idea of when a searchable database will be up and running for the government to search."). The government provided the following description of its *prospective* search protocol:

> Once items are placed in searchable formats, the search protocols proceed from the language and limitations of the search warrant. Specifically, first a search is done by date to limit the universe to dates within the chronological parameters of the search warrants creating the time relevant subset. Second, using the time relevant subset, a search of names, both individuals and businesses, is done to obtain all documents within the relevant time period that mention either a company or

> individual identified in the search warrant whose records are within the scope of the search warrant. The time relevant subset is also searched for English and Spanish words that are believed from an investigative point of view, to be relevant. For example, words relating to the crimes identified in the search warrants (e.g., cash, dinero, money, invoices, statements) have been used as a subset to search the time relevant subset. Subsequently, additional searches are conducted using search terms based upon the contents of retrieved relevant documents.

Id. After the defense pointed out that this description did not constitute a valid search protocol, Tremonte Decl., Ex. K, at 3, the government responded by restating the same description of its *planned* search protocol and adding, "This search protocol will change and has been evolving since the devices were imaged." Tremonte Decl., Ex. L, at 5.

ARGUMENT

I. Counts One, Five, and Six of the Indictment Should Be Dismissed as Duplicitous or Severed

Counts One, Five, and Six of the Indictment are duplicitous because they each charge multiple offenses within a single count. Specifically, these counts each charge conduct by the Tronix Defendants and National Defendants as jointly undertaken, even though there is no allegation suggesting that the two sets of businesses have any connection with each other; have ever coordinated or communicated with each other; have ever agreed about anything or ever mutually benefited one another; or have any business relationship with each other at all. Without more, joining such conduct in a single charge is prohibited under Federal Rule of Criminal Procedure 8(a), which requires that there be "separate counts for separate offenses" *United States v. Sturdivant*, 244 F.3d 71, 75 (2d Cir. 2001), and Rule 8(b), which "provides a more restrictive test when multiple defendants are involved." *United States v. Tureff*, 853 F.2d 1037, 1042 (2d Cir. 1988).

Rule 8 of the Federal Rules of Criminal Procedure provides:

> (a) Joinder of Offenses. The indictment or information may charge a defendant in separate counts with 2 or more offenses if the offenses charged – whether felonies or misdemeanors or both – are of the same or similar character, or are based on the same act or transaction, or are connected with or constitute parts of a common scheme or plan.
>
> (b) Joinder of Defendants. The indictment or information may charge 2 or more defendants if they are alleged to have participated in the same act or transaction, or in the same series of acts or transactions, constituting an offense or offenses. The defendants may be charged in one or more counts together or separately. All defendants need not be charged in each count.

Fed. R. Crim. P. 8.

Under Rule 8(b), "joinder is proper" only "where two or more persons' criminal acts are 'unified by some substantial identity of facts or participants' or 'arise out of a common plan or scheme.'" *United States v. Cervone*, 907 U.S. 332, 341 (2d Cir. 1990) (quoting *United States v. Attanasio*, 870 F.2d 809, 815 (2d Cir. 1989)). To determine whether such identity exists, courts look to find a "common purpose" in multiple schemes charged together in a single count. *See Attanasio*, 870 F.2d at 815. The Second Circuit has recognized that "substantial identity of facts or participants" typically means that if the defendants were tried separately, "the evidence at one trial would essentially duplicate the evidence at the other." *United States v. Feyrer*, 333 F.3d 110, 114 (2d Cir. 2003). Joinder is thus proper only where "proof of one scheme is indispensable for a full understanding of the other." *Turoff*, 853 F.2d at 1044.

Joinder is *improper*, by contrast, where "[c]omission of one of the offenses neither depended upon nor necessarily led to the commission of the other" and "proof of the one act neither constituted nor depended upon proof of the other." *United States v. Halper*, 590 F.2d 422, 429 (2d Cir. 1978). Thus, if charges against multiple defendants are not based on "the same act or transaction, or [o]n the same series of acts or transactions," both the joinder of charges and the joinder of defendants is improper. *United States v. Shellef*, 502 F.3d 82, 98 (2d Cir. 2007)

Here, there is no allegation that the National Defendants and Tronix Defendants engaged in the same acts, transactions, or series of acts and transactions; there is no allegation that the acts of one depended on or led to the acts of the other; and the proof as to each will be completely separate. Thus, Count One—the conspiracy count—improperly alleges two separate conspiracies under the guise of one in violation of these principles. Similarly, Count Five alleges structuring financial transactions by all of the defendants, when each set of defendants maintained wholly separate bank accounts and conducted financial transactions that were in no way interconnected or mutually dependent. There is no allegation that the National and Tronix Companies ever once exchanged goods, services, or currency; ever once transacted with each other; or ever once coordinated or communicated with each other about a transaction. Any alleged structuring therefore cannot be the same offense, and cannot arise from the same common scheme, and consequently Count Five runs afoul of the principles of proper joinder. Count Six is also improper, because it is predicated on Count One, and thus fails to allege interstate or foreign transportation in aid of a single money laundering conspiracy. Trial on these improperly pled charges will risk prejudice to the defendants, result in evidentiary hurdles, and lead to the possibility of a verdict that is not unanimous. Accordingly, these counts should be dismissed as duplicative, or severed.

A. Count One Alleges Multiple Conspiracies Under the Guise of One

As to Count One, it is black letter law that "an indictment may not charge multiple conspiracies in a single count." *United States v. Rigas*, 281 F. Supp. 2d 660, 664 (S.D.N.Y. 2003) (Sand, J.). Here, the conspiracy count is duplicitous because it charges two separate and distinct conspiracies – one relating to the Tronix Companies and another relating to the National Companies – as a single conspiracy. Because such duplicity in the charging instrument

prejudices the defendants and risks jury confusion, the Court should either dismiss Count One or direct the government to elect which conspiracy it will seek to prove at trial.

To determine whether a single count violates the rule against duplicity, courts focus on the "unit[] of prosecution" of the charged offense. *United States v. Dioguardi*, 332 F. Supp. 7, 21 (S.D.N.Y. 1971). Because an agreement is the "essence" of a conspiracy, *United States v. Eppolito*, 543 F.3d 25, 47 (2d Cir. 2008), the unit of prosecution for a conspiracy offense is the alleged unlawful agreement. *United States v. Rosenblatt*, 554 F.2d 36, 39 (2d Cir. 1977) ("[T]he gist of the offense remains the agreement." (internal quotation marks omitted)). "In order to prove a single conspiracy, the government must show that each alleged member agreed to participate in what he knew to be a collective venture directed toward a common goal. The co-conspirators need not have agreed on the details of the conspiracy, so long as they agreed on the essential nature of the plan." *United States v. McDermott*, 245 F.3d 133, 137 (2d Cir. 2001). Further, while "a single conspiracy is not transformed into multiple conspiracies merely by virtue of the fact that it may involve two or more phases or spheres of operation," a single conspiracy requires "sufficient proof of mutual dependence and assistance." *United States v. Maldonado–Rivera*, 922 F.2d 934, 963 (2d Cir. 1990); *accord United States v. Vanwort*, 887 F.2d 375, 383 (2d Cir. 1989) (single conspiracy exists only where the participants "mutual[ly] depend[]" on and "assist[]" each other, there is a "common aim or purpose," and "each actor [i]s aware of his part in a larger organization" (internal quotation marks omitted)).

Here, there is no connection, no coordination, and no relationship whatsoever between the two sets of companies that could conceivably meet the legal standard of a single conspiracy. The Indictment alleges that Nat owns and manages the Tronix Companies, Indictment ¶ 2, and that Abdul separately owns and manages the National Companies. *Id.* ¶ 3. The Indictment

alleges no business connection between these two sets of companies; no coordination of their business activities for mutual benefit; no mutual dependence or assistance between and among them; and no allegation whatsoever to suggest that the two sets of companies are anything other than business *competitors*. That is because there is, in fact, no connection between the two sets of companies, and the fact that they are owned by individuals who happen to be cousins and employ members of the same extended family does not establish one.[2]

Mere association—including by familial relationship—does not constitute evidence of a criminal conspiracy. *See United States v. Torres*, 901 F.2d 205, 244 (2d Cir. 1990) (approving jury instruction stating that jury "may not find that a defendant is a member in a conspiracy merely because of friendship or family relationship or association"), *abrogated on other grounds by United States v. Marcus*, 628 F.3d 36 (2d Cir. 2010). Yet, Count One indiscriminately alleges that *all* of the defendants, whether engaged in the business of the Tronix Companies or the National Companies, were involved in a single conspiracy to launder money. *See* Indictment ¶¶ 14-15. It does so without any allegation asserting that the two sets of companies mutually depend on or assist each other, or are engaged in a common aim or purpose, other than merely existing in the same market space.[3]

While the question whether there is more than one conspiracy is often a question reserved until the close of evidence, *see e.g.*, *United States v. Vanwort*, 887 F.2d 375, 383 (2d Cir. 1989), courts will address the issue at the pretrial phase where, as here, the duplicitous charge is

---

[2] As the Court is aware from our prior filings, an exhaustive analysis of the bank accounts associated with the businesses managed by Abdul and Shikeba demonstrates that there is *no relationship whatsoever* between the businesses they own and manage, and the businesses owned and managed by their cousin Nat. *See* Tremonte Decl., Ex. R.

[3] As noted above, the Indictment alleges that Rahimi was an employee of Tronix, Sysco, and National, but it does not allege any coordination or mutual benefit based on the mere fact that some of the companies happen to share a single employee.

apparent and would prejudice the defendants at trial. *See United States v. Viserto*, 596 F.2d 531, 538 (2d Cir. 1979) (where the "duplicitous character of the count appears on the face of the indictment," defendants should move "before trial to dismiss the indictment"); *United States v. Marlinga*, No. CRIM 04-80372, 2005 WL 513494, at *6 (E.D. Mich. Feb. 28, 2005) (granting defendant's motion to compel the government to reformulate the duplicitous conspiracy count); *United States v. Marcus Schloss & Co.*, 710 F. Supp. 944, 952 (S.D.N.Y. 1989) ("The requirement that a single conspiracy be alleged in the indictment permits pre-trial judicial scrutiny of the allegations' sufficiency."); *United States v. Munoz-Franco*, 986 F. Supp. 70 (D.P.R. 1997) (dismissing duplicitous conspiracy count). The Court should do so here.

Combining more than one conspiracy in one count creates a risk "that jurors will be misled into attributing guilt to a particular defendant based on evidence presented against others who were involved in a different and separate conspiratorial scheme." *United States v. Brandon*, 17 F.3d 409, 450 (1st Cir. 1994); *see also United States v. Bowline*, 593 F.2d 944, 947-48 (10th Cir. 1979) (where all defendants would be "subjected to prejudice as a result of being tried in an atmosphere where the acts and conspiracies of others [would be] introduced," dismissal of the duplicitous count is appropriate). The risk of prejudice is especially acute here, where the evidence relating to the Tronix Defendants involves allegations of bulk cash drops in hotel parking lots and other provocative allegations indicative of money laundering activity that would overwhelm and taint a jury's consideration of the National Defendants, against whom the government does not allege any such activity.

Moreover, by charging multiple conspiracies as one, the government has created an acute evidentiary problem. While co-conspirator statements are conditionally admissible against a defendant subject to independent proof that the defendant at some point was a member of

the *same* conspiracy that generates the statement, *see* Fed. R. Evid. 104(b) & 801(d)(2)(E), there is a substantial risk of mistrial if, at the close of evidence, the Court finds there were in fact *two* conspiracies, rather than one, or a likely Rule 33 motion if the jury were to find multiple conspiracies. *See United States v. Geaney*, 417 F.2d 1116, 1120 (2d Cir. 1969) (Friendly, J.) (noting difficulties of admitting co-conspirators subject to connection and determining admissibility at close of government's case depending on proof of existence of charged conspiracy). Thus, Count One should either be dismissed, or the two separate alleged conspiracies charged within it should be severed.

B. The Duplicity Inherent in Count One Infects the Other Counts That Lump Abdul and Shikeba Together with the Tronix Defendants

The problems outlined above are apparent in the manner in which the duplicity in Count One infects the other counts that charge all of the defendants *en masse*. First, it should be noted that Counts Two through Four, alleging the operation of an unlicensed money transmitting business and the failure to report CTR and IRS Forms 8300, charge only the Tronix Defendants. *See* Indictment ¶¶ 16-21. Yet Count Five charges *all* defendants with structuring financial transactions in a variety of financial institutions, including Citibank, Wells Fargo, Bank of America, Ocean Bank, and Habib American Bank. *Id.* ¶ 23. The Indictment does not allege a *conspiracy* to structure financial transactions or any interrelation of the two sets of companies' financial transactions. Indeed, the government has informed us that the alleged structured transactions pertaining to the National Defendants occurred *only* in National's Habib American Bank account and in National's account at Devon Bank not listed in the Indictment. Tremonte Decl. ¶ 24. There is no allegation—nor could there be any based in fact—that Abdul and Shikeba may be held criminally liable for any structuring in the accounts of the Tronix Defendants and *vice versa*. Indeed, as just noted, Abdul and Shikeba are *not* charged in the

counts relating to the Tronix Defendants' operation of an unlicensed money transfer business, Form 8300 violations, and CTR violations. However, because the Indictment simply joins all defendants together in a single structuring count, it creates a significant risk that the jury could convict each defendant based on the alleged, separate structuring activity of others, even when there is no identity of facts and the commission of one offense does not "depend[] upon nor necessarily led to the commission of the other." *Halper*, 590 F.2d at 429.

Finally, with respect to Count Six, that count charges interstate or foreign travel in aid of a racketeering enterprise in violation of 18 U.S.C. § 1952. Section 1952, the Travel Act, proscribes interstate travel for the purpose of facilitating or promoting certain enumerated federal and state crimes. The predicate crimes underlying the alleged Travel Act violation here are the money laundering conspiracy charged in Count One and the failure to file currency transaction reports charged in Count Three. *See* Indictment ¶ 25. But, again, as noted above, there is *no CTR allegation against Shikeba and Abdul*. Nor has the government presented any theory or evidence that Abdul and Shikeba traveled in interstate commerce or used a facility or instrumentality of interstate commerce to promote *Nat's* failure to accurately report currency transactions. While a special verdict form could potentially resolve the ambiguity as to which predicate crime supplies the basis for each defendant's conviction on Count Six as between the failure to file currency transaction reports and money laundering conspiracy, such a form would not resolve the potential lack of unanimity as to Count One. Accordingly, Count Six should be dismissed or severed in a manner consistent with the Court's resolution of Count One.

Fundamentally, the defendants have a "right not to be tried en masse for the conglomeration of distinct and separate offenses committed by others." *Kotteakos v. United States*, 328 U.S. 750, 775 (1946). Here, because the Indictment improperly combines two

different schemes under the umbrella of one conspiracy charge and multiple alleged structured transactions under the umbrella of one structuring count, Counts One, Five, and Six should be dismissed on the grounds of duplicity, *see Munoz-Franco*, 986 F. Supp. at 72, or, in the alternative, the government should be required to elect which offenses to prove at trial, *see e.g.*, *United States v. Ramirez-Martinez*, 273 F.3d 903, 915 (9th Cir. 2001) (duplicity cured if "government elects between the charges in the offending count"), *overruled on other grounds by United States v. Lopez*, 484 F.3d 1186 (9th Cir. 2007); *United States v. Hood*, 210 F.3d 660, 663 (6th Cir. 2000) (same); *United States v. Goodman*, 285 F.2d 378, 380 (5th Cir. 1960) (same).

II. The Court Should Sever the Trials of the National Defendants and the Tronix Defendants

A. The Defendants Are Misjoined Under Rule 8

As noted above, "unlike Rule 8(a), Rule 8(b) does not permit joinder of defendants solely on the ground that the offenses charged are of 'the same or similar character' . . . [Rule] 8(b) provides a more restrictive test when multiple defendants are involved." *Tureff*, 853 F.2d at 1042-43. In the present case, the Tronix and National Defendants are misjoined because there is a complete absence of common purpose and common proof among the National and Tronix Companies. *See Attanasio*, 870 F.2d at 815. None of the proof admissible against the Tronix Defendants is admissible against the National Defendants, and *vice versa*, because the Tronix and National Defendants did not share a common plan or purpose, and their alleged crimes were not part of the same act or transaction or series of acts or transactions. *See Cervone*, 907 F.2d at 341. The success of any alleged money laundering transactions by the Tronix Defendants did not depend upon or further any similar acts by the National Defendants. Nor did anything allegedly done by the National Defendants depend upon or further any similar acts by the Tronix Defendants. There is simply no substantial identity of facts or participants in the two distinct

schemes charged in the Indictment, because Abdul, Shikeba and Nat shared no common plan – and *there is no allegation that they did*. Under these circumstances, and based on the government's own allegations, the trial of National Defendants should be severed from the trial of the Tronix Defendants.[4]

B. Joinder with the Tronix Defendants Is Unfairly Prejudicial to the National Defendants

Even if the defendants and counts are properly joined in the Indictment under Rule 8, the distinct nature of the conspiracies alleged in Count One, and the volume of sensational, direct evidence implicating only one conspiracy involving the Tronix Defendants, also warrant severance of the National Defendants from the Tronix Defendants.

Rule 14 of the Federal Rules of Criminal Procedure provides, in relevant part: "If the joinder of offenses or defendants in an indictment . . . appears to prejudice a defendant or the government, the court may order separate trials of counts, sever the defendants' trials, or provide any other relief that justice requires." Fed. R. Crim. P. 14. The Supreme Court has held that a severance should be granted under Rule 14 "if there is a serious risk that a joint trial would compromise a specific trial right of one of the defendants or prevent the jury from making a reliable judgment about guilt or innocence." *Zafiro v. United States*, 506 U.S. 534, 539 (1993). In *Zafiro*, the Supreme Court found that "[s]uch a risk might occur when evidence that the jury should not consider against a defendant and that would not be admissible if a defendant were tried alone is admitted against a codefendant. For example, evidence of a codefendant's

[4] The presence of a single defendant who was an employee of companies on both sides of the case is insufficient to render joinder proper. *See United States v. McCabe*, No. 05-CR-0237(S-1)(DRH), 2006 WL 2990480, at *2 (E.D.N.Y. Oct. 19, 2006) (presence of lead defendant in all counts was "clearly an insufficient predicate for joinder" in the absence of "some type of overarching link between" schemes alleged in the indictment).

wrongdoing in some circumstances erroneously could lead a jury to conclude that a defendant was guilty." *Id.*

Consequently, the Second Circuit has held that severance for separate trials is warranted where "the sheer volume and magnitude of the evidence against one defendant so dwarfs the proof presented against his co-defendant[s] that a severance is required to prevent unacceptable spillover prejudice." *United States v. Spinelli*, 352 F.3d 48, 55 (2d Cir. 2003). In *United States v. Branker*, 395 F.2d 881 (2d Cir. 1968), the Second Circuit held that severance is warranted when a joint trial will cause the jury to hear evidence of "incidents of criminal misconduct which do not involve these defendants in any way," such that there is a "huge volume of testimony relating not to [the defendants] but to the manifold criminal activities of [their co-defendants]." *Id.* at 888; *accord United States v. Kelly*, 349 F.2d 720, 759 (2d Cir. 1965) (holding defendant was unacceptably prejudiced by "the slow but inexorable accumulation of evidence of fraudulent practices by [his] co-defendants," where "some of this rubbed off on [defendant]"). Similarly, in *United States v. Gilbert*, 504 F. Supp. 565 (S.D.N.Y. 1980), a court found severance to be warranted based on the "substantial risk that [defendant] would be prejudiced by the gradually accumulating effect of evidence of [his codefendant's] wrongdoing, . . . in connection with transactions where [defendant] played no part, or where his involvement was directed by others without full disclosure to [defendant]," and where there was a risk that the jury would be unable to distinguish between the respective roles of the various alleged co-conspirators. *Id.* at 571.

Here, there is no business connection between the Tronix Defendants and the National Defendants, and no evidence to suggest that the business dealings of Nat were in any way known or reasonably foreseeable to Abdul and Shikeba. Thus, if tried together, Shikeba and Abdul will be forced to defend themselves at a trial in which extensive evidence of "incidents of criminal

misconduct which do not involve [them] in any way" is put before the jury. *Branker*, 395 F.2d at 888. That evidence is certain to be highly prejudicial, because unlike the purely circumstantial case the government will put on as to Abdul and Shikeba, the case against Nat will involve direct, sensational evidence that the jury will in all likelihood attribute to all defendants across the board, regardless of their involvement in the conduct at issue. *See Gilbert*, 504 F. Supp. at 571 (severance warranted due to "substantial risk that [defendant] would be prejudiced by the gradually accumulating effect of evidence of [codefendant's] wrongdoing . . . in connection with transactions where [he] played no part").

For example, the search warrant application alleges that Nat "sent large amounts of cash through the mail from Long Island to Miami to be deposited in structured amounts." Tremonte Decl. Ex. D, ¶ 18. It further alleges that Nat "specifically provided instructions to individuals on how to deposit the currency he sent to them." *Id.* It also states that on February 27, 2018, an undercover agent for the Department of Homeland Security met with Nat at a hotel and handed him $75,000 in purported drug proceeds separated into eight bundles and concealed in a Nike shoebox wrapped in a white plastic bag. *Id.* ¶ 52. No such allegations have been made against Abdul and Shikeba, whose trial will exclusively involve evidence that the National Companies received a small fraction of payments alleged to be drug proceeds (the forensic accounting analysis submitted to the Court has confirmed it is only a fraction, *see* Tremonte Decl., Ex. R), and the government will contend that they did so knowingly because they operated businesses that, at times, received payments on invoices from third parties. Because the alleged evidence of Abdul and Shikeba's knowledge will be highly circumstantial, alleged evidence of Nat's direct receipt of cash known to be drug proceeds has the potential to overwhelm and prejudice the jury against all defendants—especially those that are related to each other by blood.

Similarly, "[t]he risk of prejudice against a defendant due to a joint trial may be heightened where, for example, many defendants are tried together in a complex case and they have markedly different degrees of culpability." *United States v. Shkreli*, 260 F. Supp. 3d 247, 253 (E.D.N.Y. 2017) (internal quotation marks omitted). Here, no less than *seven* defendants are currently scheduled to go trial jointly, a situation that will necessarily lead to juror confusion, a chaotic courtroom atmosphere with multiple overlapping objections and extended sidebars, and an unacceptably high risk of substantial prejudice to Abdul and Shikeba because the "sheer volume and magnitude" of evidence against the Tronix Defendants simply "dwarfs the proof presented against" them. *Spinelli*, 352 F.3d at 55. Thus, severance is warranted in light of the "substantial risk that [Abdul and Shikeba] would be prejudiced by the gradually accumulating effect of evidence" of wrongdoing in which they "played no part." *Gilbert*, 504 F. Supp. at 571.

Moreover, the very number of co-defendants going to trial, the volume of evidence against the Tronix defendants, and the complexity of the case will both confuse the jury and undercut any gains in judicial economy that would derive from trying the cases jointly. In *Shkreli*, which involved only *two* defendants, Judge Matsumoto expressed concern about the efficiency of the trial because "both defense counsel have indicated they expect to raise frequent objections during trial, both to the government's and each co-defendant's evidence, leading to a litany of side bar debates about various legal issues including limiting instructions." *Shkreli*, 260 F. Supp. 3d at 256. Such a situation, the court held, would "disrupt the flow of the trial and increase the length of the trial, will likely confuse the jury in what is already a complex case, and may risk prompting the jury to find both defendants guilty based on each defendant's arguments that he was deceived by the other, instead of deciding the case based on the evidence presented." *Id.*

Here, similarly, multiple overlapping objections, extensive side-bars, and juror confusion are likely to result from a joint trial, especially if the conspiracy count is permitted to be tried as a single charge. As noted above, unless dismissed or severed, that count will create substantial evidentiary challenges in terms of determining which co-conspirator statements are admissible against which defendants. A joint trial thus poses a high risk of prejudice to the National Defendants and little in the way of efficiency. Thus, even if trying all of the defendants together would be efficient—which is a highly dubious proposition given the complexity and chaos of trying the case against seven co-defendants with substantially different roles in distinct alleged schemes and all raising substantially different issues to be decided by the Court and the jury—any marginal increase in judicial economy must "give way to fairness," and "from a trial management perspective and to prevent substantial prejudice and jury confusion, severance is warranted." *Id.* at 256-57. The Court should accordingly sever the trials of the National Defendants and the Tronix Defendants.

III. The Court Should Suppress the Fruits of the Searches of National's Office and Abdul and Shikeba's Homes

The Court should suppress the fruits of the searches of National's office in Farmingdale, New York, and Shikeba and Abdul's homes in Farmingdale and Syosset, New York, respectively. These searches were based on warrants that violated the Fourth Amendment's particularity requirement, were overbroad, and did not allege probable cause that evidence of a crime would be found in Shikeba and Abdul's homes. Moreover, the evidence should be suppressed because the government waited for nearly *ten months* before beginning to search the

electronic devices recovered during the searches and did so without a search protocol that limited in any meaningful way the scope of the search.

A. The Warrants Here Violated Fourth Amendment Requirements

1. *The Particularity Requirement and Prohibition Against Overbreadth*

To prevent "general, exploratory rummaging in a person's belongings," *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971), the Warrants Clause of the Fourth Amendment "requires particularity and forbids overbreadth," *United States v. Jacobson*, 4 F. Supp. 3d 515, 521 (E.D.N.Y. 2014) (Bianco, J.) (internal citation and quotation marks omitted). A warrant's "description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based." *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013). "Courts implement the particularity requirement by insisting that warrants not 'leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized.'" *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 453 (S.D.N.Y. 2013) (quoting *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990)). Put differently, "a warrant must be sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal quotation marks and alterations omitted).

The Second Circuit has held that, under the particularity requirement, a warrant must (1) identify the specific offense for which there is probable cause; (2) describe the place to be searched; and (3) specify the items to be seized in relation to the designated crimes. *See United States v. Ulbricht*, 858 F.3d 71, 98–99 (2d Cir. 2017); *Galpin*, 720 F.3d at 445-46. Moreover, the Supreme Court has held that the Fourth Amendment "requires particularity in the warrant, not in the supporting documents," and, accordingly, "the fact that the warrant *application*

adequately described the 'things to be seized' does not save the *warrant*." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). Numerous courts have held that the absence of a date limitation in a warrant, while not necessarily dispositive, reflects strong indicia of the warrant's lack of particularity. *See, e.g.*, *Zemlyansky*, 945 F. Supp. 2d at 459-60 (collecting cases); *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *23 (S.D.N.Y. Apr. 4, 2007) (warrant's "lack of particularity is only compounded by the absence of any date restriction on the items to be seized"); *United States v. Costin*, No. 5 Cr. 38, 2006 WL 2522377, at *12 (D. Conn. July 31, 2006) ("A warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular.").

The Fourth Amendment's prohibition against overbreadth is "necessarily tied" to the particularity requirement because "limiting the authorization to search to the specific areas and things for which there is probable cause to search . . . ensures that the search will be carefully tailored to its justifications." *In re 650 Fifth Ave. & Related Properties*, 830 F.3d 66, 99 (2d Cir. 2016). In determining whether a warrant is overbroad, courts focus on "whether there exists probable cause to support the breadth of the search that was authorized." *Zemlyansky*, 945 F. Supp. 2d at 464. Where a warrant offers only an "unparticularized description of the items subject to seizure," such a description "may cause it to exceed the scope of otherwise duly established probable cause." *United States v. Wey*, 256 F. Supp. 3d 355, 382 (S.D.N.Y. 2017).

2. *The Warrants Are Facially Invalid Because They Authorize the Seizure of an Unrestricted Range of Documents and Devices without Limitation*

As previously described, the warrants here authorized the seizure of all books and records related to any one of the premises to be searched; all records in the names of or relating to numerous individuals and companies; and all computers and electronic devices—without any date limitation. This invitation for an exploratory rummaging violates foundational Fourth

Amendment principles requiring particularity and forbidding overbreadth. *See, e.g., United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant authorizing "seizure of virtually every document and computer file" at an office "failed to describe with particularity the items to be seized"); *United States v. Dale*, 991 F.2d 819, 846 (D.C. Cir. 1993) (warrant authorizing seizure of "essentially all of [the business's] records after [a specified date] … was not sufficiently particular"); *Vilar*, 2007 WL 1075041, at *24 (warrant reflected "patent lack of particularity," notwithstanding illustrative list of items, where catch-all language in warrant authorized seizure of "any corporate record . . . regardless of date or subject matter").

The warrants here do not incorporate the application or supporting affidavit by attachment or reference. *See* Tremonte Decl., Exs. E, F, G. Instead, each warrant simply authorizes a search of the premises with "Attachment H" as the only document guiding the agents' discretion as to what items to search and seize. The description in Attachment H, however, includes broad categories of documents relating to *the subject premises themselves*. This creates a circularity that allows for the executing agents' unbridled discretion to pick and choose documents that appear of interest but are not tethered to any probable cause. Moreover, Attachment H invites the agents to seize any documents in the name of the defendants, another way in which the warrant permits searching of essentially any document found in the course of the search. Attachment H places no restriction at all on the seizure and search of electronic devices. This provision is especially troubling when it comes to the defendants' homes because the warrants "did not stop with any devices owned by" Shikeba and Abdul, but rather "broadly authorized seizure of *all* cell phones and electronic devices, without regard to ownership." *United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (holding warrant was overbroad on that basis). Consequently, the agents seized several computers and iPods belonging to

Shikeba's minor children, returning them after a demand from the defense. Tremonte Decl. ¶ 14. Finally, the warrants contain no date limitation cabining the records to be seized to the time-period alleged as being the span of the conspiracy. *See Vilar*, 2007 WL 1075041, at *23 (warrant's "patent lack of particularity is only compounded by the absence of any date restriction on the items to be seized").

The warrants here bear critical similarities to the warrants found to be defective in *United States v. Wey*. Although the warrants in that case had the additional deficiency of failing to include even the statutory offenses being investigated, Judge Nathan was especially troubled by the warrants' authorizing the seizure of broad "buckets of material" including "financial records" and "communications" relating to entities and individuals listed in a separate exhibit, which included the defendant himself. 256 F. Supp. 3d at 386. This formulation, Judge Nathan held, failed to provide "any practical tool to guide the searching agents in distinguishing meaningfully between materials of potential evidentiary value and those obviously devoid of it" and thus rendered the warrants effectively general warrants. *Id.* In addition, Judge Nathan cited the absence of a date limitation in the warrants, holding that "the 'absence of such a limit reinforces the Court's conclusion' that the Warrants are insufficiently particularized." *Id.* at 388 (quoting *Zemlyansky*, 945 F. Supp. 2d at 459-60).

Here, similarly, although Attachment H identified the crimes being investigated, it authorized the search and seizure of "[a]ny and all business books and records relating to the Subject Premises" and "[a]ny and all records in the names of" the defendants, thus permitting an "exploratory rummaging in [Abdul and Shikeba's] belongings" to find evidence of those crimes. *Galpin*, 720 F.3d at 445 (internal quotation marks omitted). Attachment H placed *no* limits on the broad authorization to search and seize all electronic devices—an invitation for a general

fishing expedition through Abdul and Shikeba's personal computers and other storage media, as well as personal computers and storage media belonging to persons—including children—not involved in the events described in the indictment and the Szwalek Affidavit. *See Wey*, 256 F. Supp. 3d at 386-87 (noting that the warrants' lack of particularity was "exacerbated by the fact that the Warrants target, in significant measure, the contents of electronic devices, such as computers, internal and external hard drives, and smart phones"); *see also Ulbricht*, 858 F.3d at 99-100 (noting that risk that "every warrant for electronic information will become, in effect, a general warrant" unless the warrant places "meaningful parameters on an otherwise limitless search of a defendant's electronic media"). Finally, like the warrant in *Wey*, the warrants here "did not set out any date ranges or other timeframe-based criteria." *Wey*, 256 F. Supp. 3d at 365.

Because the warrants here placed no constraints on the places to be searched and items to be seized, no explanation of how those items might relate to the charged crimes, and no limitation whatsoever on the seizure and search of electronic devices and storage media, they failed to meet the Fourth Amendment's particularity requirement and thus were facially invalid. Moreover, absence of probable cause to support the breadth of the warrant independently renders them invalid. *See In re 650*, 830 F.3d at 99. Accordingly, the Court should suppress the fruits of the search warrants. [5]

[5] The facial insufficiency of the warrants precludes the government from invoking the good faith exception here to limit the application of the exclusionary rule. *See United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (good faith exception does not apply "where the warrant is so facially deficient that reliance upon it unreasonable").

3. *The Warrant Application Failed to Satisfy the Probable Cause Standard as to Shikeba and Abdul's Homes*

In addition to the defects in the warrants outlined above, the warrants' authorizations to search the homes of Abdul and Shikeba are unsupported by probable cause. Accordingly, any evidence obtained from those locations should be suppressed.

The warrant application describes broadly the "Khwaja family companies," failing to distinguish in any way between the National Companies and the Tronix Companies. Tremonte Decl., Ex. D, at ¶ 11. It states, again without differentiation, that both groups of companies receive "bulk currency derived from illegal drug proceeds and other illicit moneys in South America" and that the "KHWAJA COMPANIES[']bank accounts [are] used to fund the TBML [trade-based money laundering] scheme." *Id.* ¶ 12. The application states that "the employees of the KHWAJA COMPANIES whose residences are sought to be searched . . . routinely conduct their work, including TBML work, at home," and then states—in highly misleading fashion—"[b]ulk currency has been delivered to and stored in some of these locations, in particular [Nat's] home" and "[t]his currency is then distributed into and among the KHWAJA COMPANIES." *Id.* ¶ 15. The application does not disclose that money from Nat, whether in bulk currency or otherwise, was *never* transferred to Abdul, Shikeba, or the National Companies, and does not reveal the fact that neither Abdul nor Shikeba nor the National Companies ever received bulk currency. "It is well established that probable cause must exist as to the particular individual under suspicion, and not simply others in whose company he may have been." *United States v. Gonzalez*, No. 86 CRIM. 1057 (WCC), 1987 WL 6923, at *2 (S.D.N.Y. Feb. 6, 1987). The warrant application's failure to establish probable cause specific to Abdul and Shikeba is fatal to their adequacy under the Fourth Amendment.

The same failure to disclose the distinction between the National Companies and Tronix Companies infects other aspects of the warrant application. The application states that the "KWHAJA COMPANIES . . . received millions of dollars in cash," and such cash "was deposited on successive days in amounts less than $10,000 to evade the Bank Secrecy Act reporting threshold." Tremonte Decl., Ex. D ¶ 18. The application then goes on to describe structured deposits made exclusively by *Nat*, with no evidence of any structuring by Shikeba or Abdul, or by anyone else for that matter in the bank accounts of the National Companies.

With respect to the specific homes, the application asserts that Shikeba was intercepted on various phone calls conducting business of Wireless Hub and Gotham Discounts—two companies *not* included in the Indictment but which, the application states (without any factual support) are "part of the TBML scheme"—from her home in Farmingdale. *Id.* ¶ 65. The application also states that "bank records" are sent to Shikeba's home for a "Habib American" account, and states, vaguely and in purely conclusory terms, that "[t]hese accounts have business funds from the Khawaja COMPANIES funnel through them." *Id.* ¶ 68. The application does not state which businesses the accounts are for, or why, having obtained them through Grand Jury subpoenas, an additional search of Shikeba's home was necessary to obtain the very same bank records.

As to Abdul's home, the application similarly states that Abdul lives there, "numerous bank records of accounts involved in the KHWAJA MLO are mailed" there, and that Abdul "has financial records and business records" at his home. *Id.* ¶ 80. The application re-states that Abdul is the owner of National, and quotes Whatsapp communications between Abdul and others regarding the business of National, though without any connection to his residence. *See id.* ¶¶ 85-87.

Simply put, the bare statement that a defendant lives at a particular residence, speaks on the telephone from there, and receives bank statements—which, based on the assertions in the application are just as likely of a personal nature as related to the businesses in question—is insufficient to justify a search warrant of the residence. The Supreme Court has held that an arrest warrant, while providing limited authority to enter a defendant's home to secure his arrest, does not confer the right to search the home. *See Steagald v. United States*, 451 U.S. 204, 216 (1981). Instead, the warrant requirement of the Fourth Amendment demands particularized facts that indicate evidence of a crime will be found *in the location* to be searched. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983) (probable cause determination requires "fair probability that contraband or evidence of a crime will be found in a particular place"). "Those concerns about the distinct requirements for a search warrant are particularly salient" where, as here, "the warrant application sought authorization to search a home, which stands at 'the very core' of the Fourth Amendment's protections." *Griffith*, 867 F.3d at 1271 (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)). Because the warrant application contains no such information regarding the homes, the warrant is unsupported by probable cause as to those locations. The evidence obtained from Abdul and Shikeba's homes should accordingly be suppressed.[6]

4. *The Search of Shikeba's Home Violated Rule 41*

Unguided by any limitation in the warrant, the agents' search of Shikeba's home was a blunderbuss search that swept up documents and electronic devices unauthorized by the warrant. In addition, the search was conducted in contravention of Rule 41. The agents took the

[6] The misleading nature of the allegations lumping together all of the "Khwaja companies" in the warrant application separately vitiates the good faith exception. *See Clark*, 638 F.3d at 100 (good faith exception does not apply where "the issuing magistrate has been knowingly misled").

passports, birth certificates, and social security cards of Shikeba's husband and children, Shikeba and her husband's marriage certificate, laptops and iPads belonging to Shikeba's children that the children used for their schoolwork, and business records pertaining to Shikeba's husband's art gallery. *See* Tremonte Decl. ¶ 16 & Ex. H. The agents failed to provide Shikeba with a copy of the warrant and did not leave an inventory of the items they seized, in violation of the requirements of Federal Rule of Criminal Procedure 41(f)(1)(B) and (C).

While a Rule 41 violation does not necessarily rise to the level of "constitutional magnitude," it requires suppression where "(1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if [Rule 41] has been followed or (2) there is evidence of intentional and deliberate disregard of a provision in [Rule 41]." *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975). Here, the combination of facts regarding the manner in which the search was conducted suggests intentional and deliberate disregard of the Rule, and, at a minimum, the Court should order a hearing on that question.

5. *The Government Failed to Search the Seized Electronic Devices Promptly and Its Ultimate Search of the Devices Was an Unguided Fishing Expedition*

Even assuming *arguendo* that the warrants properly authorized the seizure of evidence from the defendants' offices and homes, the Court should suppress evidence from the electronic devices seized because the government sat on its hands for months after seizing the devices, searching them only when defense counsel made a demand for their return. Further, the government's "search protocol," which it provided to the defense and the Court by letter dated June 14, 2019, was no search protocol at all, and instead allowed for a generalized fishing expedition through dozens of the defendants' electronic devices. These deficiencies compel suppression of the evidence seized on the electronic devices.

i. Failure to Search Electronic Devices

In *United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012), the government seized numerous electronic devices for off-site searching, promptly imaged the electronic devices and returned the originals to their owners. *See id.* at 209-10. The government then sought and obtained search warrants to review the images of the materials. *Id.* Rather than promptly conduct the search, however, approximately fifteen months passed between the government's execution of its original search warrant—and taking of the electronic devices—and the filing the defendant's motion to suppress, at which the time the government appeared not to have conducted a review of the evidence seized and imaged to determine whether any of the imaged evidence fell outside the scope of the original warrant. *Id.* at 210. Judge Irizarry held that the government's failure to begin its review of the data for fifteen months was "unacceptable and unreasonable" and accordingly a violation of the Fourth Amendment. *Id.* at 215. Although few cases had, up to that point, set limits on the amount of "reasonable time" the government had to conduct a review of materials seized for off-site review, Judge Irizarry held that the government's "flagrant[] disregard" of its obligation to promptly review the material to determine what was within and without the scope of the search warrant required blanket suppression of the evidence. *Id.* at 215-16 (internal quotation marks omitted).

Similarly, in *United States v. Debbi*, 244 F. Supp. 235 (S.D.N.Y. 2003), the government seized numerous boxes of documents from the defendant's home, but failed to search them to determine which materials were within or without the scope of the warrant until, eight months later, "after repeated demands from defense counsel," the government searched the materials and returned those deemed irrelevant to the case. *Id.* at 237-38. Judge Rakoff ordered suppression of any materials that were not evidence of the charged offenses, and ordered a hearing on whether

blanket suppression was warranted. *See id.* at 238. The government ultimately consented to suppression as to all items seized from the defendant's home that the government contended were evidence of the charged offenses. *See United States v. Debbi*, No. 02 CR. 808(JSR), 2003 WL 1922928, at *1 (S.D.N.Y. Mar. 31, 2003).

Here, the government seized dozens of electronic devices from the defendants on November 15, 2018. At a court conference some seven months later, the Court ordered the government to provide its search protocol for the data from those electronic devices. Tremonte Decl. ¶ 18. In response, the government filed a letter dated June 14, 2019, stating that "the material needs to be placed in a searchable format and this frequently requires the creation of a virtual environment. That virtual environment requires software programs and licenses which often must be purchased." Tremonte Decl., Ex. J, at 2. The letter then stated, "[D]elivery of some such software programs to use in furthering the extraction of the relevant data are being received next week . . . . After the use of those programs, the government will have a better idea of when a searchable database will be up and running for the government to search." *Id.* In other words, the government acknowledged that seven months after it seized the electronic devices, it had not begun searching them.[7] It is unknown when, after that point, the government began to search the devices, but the defense received an initial tranche of discovery from the search warrant returns some three months later—*i.e.*, ten months after the seizure of the devices—on September 16, 2019. *See* Tremonte Decl., Ex. M (Sept. 16, 2019 Discovery Letter).

[7] The government filed a subsequent letter protesting that it had begun searching the electronic devices much earlier, but describing in concrete terms only the *imaging* of such devices, not searching. *See* Tremonte Decl., Ex. K, at 3-4. The undersigned requested a hearing at that time to determine when the government actually began its search and renews that request here.

The government's failure to search the devices for at least seven—and perhaps up to ten—months, and doing so only after repeated requests by the defense both directly to the government and for Court intervention, demonstrates "flagrant[] disregard" of its obligation and warrants suppression, *Metter*, 860 F. Supp. 2d at 215 (internal quotation marks omitted), or, at a minimum, a hearing so that the Court can determine when the government began its search, *see Debbi*, 244 F. Supp. at 238; *see also United States v. Lumiere*, No. 16 Cr. 483, 2016 WL 7188149, at *3 (S.D.N.Y. Nov. 29, 2016) (denying suppression after evidentiary hearing after evidentiary hearing to determine whether government conduct was similar to "extreme circumstances discussed in *Metter*").

ii. Absence of Search Protocol

On May 10, 2019, nearly six months after it has seized the defendants' electronic devices, the government indicated by letter that it was making available discovery from those devices. What the government disclosed, however, turned out to be mirror images of the devices, *i.e.*, the government simply copied and produced the entire contents of the devices seized. *See* Tremonte Decl., Ex. I. On June 7, 2019, counsel for Abdul requested that the government provide its "search review protocol or other procedure it used to review the[] 8 terabytes of digital content." *Id.* At a court conference on June 13, 2019, the Court ordered the government to provide such a search protocol. *See* Tremonte Decl. ¶ 18. The following day, June 14, 2019, the government sent defense counsel a letter purporting to provide a protocol for searching the electronic devices. *See* Tremonte Decl., Ex. J. But, in fact, the proposed search protocol provided by the government placed no real limits on the its ability to rummage through the entirety of the electronic data it had seized in the hopes of finding some evidentiary morsel. That is a mode of

searching that the Fourth Amendment forbids. *See Coolidge*, 403 U.S. at 467 (Fourth Amendment prohibits "general, exploratory rummaging").

"The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous. This threat is compounded by the nature of digital storage." *Galpin*, 720 F.3d at 447; *accord Ulbricht*, 858 F.3d at 99 (electronic data poses "especially potent threat to privacy"). A search protocol is the only way the government can ensure compliance with the Fourth Amendment's requirements while sifting through the vast reams of data that can be stored on modern-day digital devices. *See Galpin*, 720 F.3d at 451 (stating that it is advisable for government to use such a search protocol if it wishes to invoke the plain view doctrine); *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (requiring use of search protocol). But here the government's purported search protocol simply amounted to an assertion that it would rummage through the defendants' electronic devices in a search for material responsive the warrant. *See* Tremonte Decl., Ex. J. Its explanation of *how* it would conduct the search made clear that it had imposed no real limitation on itself.

For example, the government stated it had created a subset of the data based on the "chronological parameters of the search warrants." *Id.* at 5. But, as noted above, the warrants themselves contained no date limitation. *See, e.g.*, Tremonte Decl., Ex. D. Further, if the government indeed has searched all of the electronic data, or even a subset, for each of the defendants' names and the names of their companies, that is precisely the overbreadth problem that the court identified in *Wey*, 256 F. Supp. 3d at 386. The search terms the government proposed to use—"cash, dinero, money, invoices, statements," Tremonte Decl., Ex. J at 2, were guaranteed to turn up as much non-responsive material as responsive material. They are terms

that are likely to capture every record kept on hand by a business engaged in commerce, and therefore do nothing to limit the agents' search to the scope of probable cause. Finally, the government expressly stated that it may change the search protocol at any time, forswearing any limitation the protocol placed on the agents. *See* Tremonte Decl., Ex. L.

Simply put, the foregoing does not articulate a real search protocol and does not limit the government's ability to view any file on the electronic devices. A search protocol is a detailed explanation by the government of "*how* it is going to conduct this search to minimize the risk that files outside the scope of the warrant will be discovered." *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 168 (D.D.C. 2014) (emphasis added). Simply stating that the search will adhere to the scope of the warrant does not explain how the search will be conducted to accomplish that goal. While a keyword search can be "a useful step in the right direction" it "still do[es] not actually give the Court a *search protocol*," *i.e.*, a "technical explanation of how the government intends to conduct the search so that the Court may conclude that the government is making a genuine effort to limit itself to a particularized search." *Id.*; *see also United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) ("Officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant."). To the extent the government conducted its search based on the vague and generalized criteria set forth in the government's June 14, 2019 letter, it engaged in the kind of exploratory rummaging the Fourth Amendment forbids. Accordingly, the Court should suppress evidence from the electronic devices or, at a minimum, order a hearing at which the government will finally be compelled to explain—as the Court had previously ordered—the manner in which it conducted the search of the electronic devices under oath.

IV. The Court Should Suppress the Fruits of the Wiretap Or, in the Alternative, Order a *Franks* Hearing

The fruits of the wiretap, too, should be suppressed. Contrary to statutory requirements, the wiretap application contains no allegation as to the necessity of a wiretap on Shikeba and Abdul's phones. Further, the sworn affidavit supporting the application omitted critical, material information, concealing it from the then-district judge. Had such material information been included the wiretap would not have been authorized. Accordingly, the Court should suppress the fruits of the wiretap or, in the alternative, order a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

A. A Wiretap Should Only Be Authorized Based on a Full and Complete Showing of Probable Cause and Necessity, and Agents Conducting a Wiretap Must Take Care to Ensure the Privacy of Its Targets

A wiretap is "the greatest of all invasions of privacy." *Berger v. New York*, 388 U.S. 41, 58 (1967) (Douglas, J., concurring). "It places a government agent in the bedroom, in the business conference, in the social hour, in the lawyer's office – everywhere and anywhere a 'bug' can be placed." *Id.* at 64-65. Given the intrusiveness of a wiretap, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 87 Stat. 197, 18 U.S.C. §§ 2510–2520 ("Title III"), authorizing "the interception of private wire and oral communications . . . only when law enforcement officials are investigating specified serious crimes and receive prior judicial approval, an approval that may not be given except upon compliance with stringent conditions." *Gelbard v. United States*, 408 U.S. 41, 46 (1972). Because of the extraordinary nature of a wiretap, Congress required the government to provide a "full and complete statement of the facts and circumstances relied upon by the applicant." 18 U.S.C. § 2518(1)(b). This

requirement is meant to ensure that "careful judicial scrutiny" is applied before a wiretap is authorized. *United States v. Gigante*, 538 F.2d 502, 506 (2d Cir. 1976).

Title III also requires a demonstrated showing that a wiretap is *necessary*, and a "full and complete statement" of the "investigative procedures [that] have been tried" and the reasons those procedures would "be unlikely to succeed." 18 U.S.C. § 2518(1)(c). Further, the judge may authorize the wiretap only "if the judge determines on the basis of the facts submitted by the applicant that," among other requirements, "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c). "Taken together, §§ 2518(1)(c) and (3)(c) require a full and complete statement establishing necessity" of the wiretap. *United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001). The Second Circuit has "emphasized that 'generalized and conclusory statements that other investigative procedures would prove unsuccessful' will not satisfy Title III." *United States v. Concepcion*, 579 F.3d 214, 218 (2d Cir. 2009) (quoting *United States v. Lilla*, 699 F.2d 99, 104 (2d Cir. 1983)). The purpose of this rule is to support Congress' "clear intent to make doubly sure that the statutory authority be used with restraint." *United States v. Giordano*, 416 U.S. 505, 515 (1974). "The plain effect of the detailed restrictions of [the statute] is to guarantee that wiretapping or bugging occurs only when there is a genuine need for it and only to the extent that it is needed." *Dalia v. United States*, 441 U.S. 238, 250 (1979).

Finally, Title III expressly requires that every wiretap order "contain a provision that the authorization to intercept . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." 18 U.S.C. § 2518(5). This provision "instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations," *Scott v. United States*, 436 U.S. 128, 140

(1978), in order to "ensure that unnecessary intrusions into the private lives of its targets [a]re kept to a minimum." *United States. v. Goffer*, 756 F. Supp. 2d 588, 595 (S.D.N.Y. 2011). Where calls of more than two minutes in length are persistently recorded, even though the calls contain no pertinent information, the agents monitoring the calls have failed to minimize their interceptions properly. *See United States v. Capra*, 501 F.2d 267-76 (2d Cir. 1974); *Zemlyansky*, 945 F. Supp.2d at 478.

Although, in ordinary circumstances, a "reviewing court must afford considerable deference to the probable cause determination of the issuing" judge, *Walczyk v. Rio*, 496 F.3d 139, 157 (2d Cir. 2007), "little or no deference is due where the government's affidavit misstated or omitted material information." *United States v. Rajaratnam*, No. 09 CR 1184 RJH, 2010 WL 4867402, at *7 (S.D.N.Y. Nov. 24, 2010) ("*Rajaratnam I*") (citing *United States v. Canfield*, 212 F.3d 713, 717 (2d Cir. 2000)). Where misstatements or omissions in a wiretap application are alleged, courts apply the standard set forth in the Supreme Court's decision *Franks v. Delaware*, 438 U.S. 154 (1978). *See United States v. Rajaratnam*, 719 F.3d 139, 151 (2d Cir. 2013) ("*Rajaratnam II*"). The *Franks* framework requires the defendant to make a preliminary showing that "(1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge's probable cause or necessity finding." *Id.* at 146 (internal quotation marks and alterations omitted).[8]

[8] "Title III contains its own exclusionary rule." *United States v. Bianco*, 998 F.2d 1112, 1125 (2d Cir. 1993). No intercepted communications "and no evidence derived therefrom may be received in evidence in any trial . . . if the disclosure of that information would be in violation of [Title III]." 18 U.S.C. § 2515. Because Title III contains its own, statutory exclusionary rule, suppression is "not limited to constitutional violations." *Giordano*, 416 U.S. at 527. Rather, suppression is required whenever "there is failure to satisfy any of those statutory requirements

B. The Wiretap Application Failed to Establish the Necessity of a Wiretap as to Abdul and Shikeba

The Szwalek Affidavit supporting the wiretap application of August 30, 2017—the first iteration of the application in which Shikeba and Abdul were listed as subject individuals—contains thirty-three paragraphs of allegations regarding alternative investigative techniques that have failed or appear likely to fail in order to establish the necessity requirement of Title III. Not one of these paragraphs alleges a single concrete fact to establish necessity as to Shikeba and Abdul.

The necessity section of the Affidavit describes in detail the information learned from prior interceptions regarding Nat's trafficking of bulk currency, Tremonte Decl., Ex. B, ¶ 99; the shipping of cash via Federal Express from Nat to Melendez Maynor and his instructions to deposit the cash into Tronix accounts, *id.*; the inability of undercover agents to penetrate the money laundering organization ("MLO") of Nader Farhat and his "key associates such as [Nat]," *id.* ¶ 101; the limitations of physical surveillance of Nat because of his international and domestic travel and because he and Rahimi live in the same residential development, *id.* ¶¶ 104-05, 107; the fact that CBP's financial investigations would not reveal the operations of the Farhat MLO because of the way in which financial transactions are structured by Tronix employees, *id.*

---

that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." *Id.* Importantly, the good faith exception set forth in *United States v. Leon*, 468 U.S. 897 (1984), does not apply to wiretap orders issued improperly under Title III. *See United States v. Rice*, 478 F.3d 704, 712–14 (6th Cir. 2007) (holding that "[t]he language and legislative history of Title III strongly militate against engrafting the good-faith exception into Title III warrants."). The Second Circuit has never held to the contrary. While the Circuit recently reversed suppression of a wiretap in a case where the misstatements in support of the wiretap application were unintentional, the court did not rest its holding on that ground, but rather held that the misstatements did not, under the particular circumstances in that case, render the wiretap unlawful under Title III and that the district court erred in failing to apply the *Franks* standard. *United States v. Lambus*, 897 F.3d 368, 395-98 (2d Cir. 2018).

¶ 112; the unviability of using pole cameras to gather evidence near Nat's residence, *id.* ¶ 115; the use of toll records to obtain information about the calling habits of Nat and employees and associates of Tronix, *id.* ¶¶ 117, 119; a Grand Jury subpoena that was served on Federal Express for all shipments between Nat and the Tronix office in Miami, *id.* ¶ 126; and the difficulty of conducting trash searches on Nat because he and other subject individuals live in close proximity to one another, *id.* ¶ 127. Whether or not these allegations are sufficient to support a finding of necessity as to Nat—a question on which we take no position—they do nothing to establish necessity as to Abdul and Shikeba. Nowhere in these allegations does the affidavit adduce facts to support a connection between Nat or the Tronix Companies on the one hand and Abdul, Shikeba, and the National Companies on the other that could support a finding of necessity as to the latter (nor could it, for the reasons outlined above).

Indeed, the only paragraph regarding necessity that does mention Shikeba and Abdul states that agents *successfully* conducted searches of their electronic devices when they were crossing the border at John F. Kennedy International Airport. *Id.* ¶ 111. The paragraph goes on to state that the agents have not done so with respect to Nat because of concerns that such a border search would "raise . . . suspicions." *Id.*[9] The paragraph goes on to state, in general, boilerplate fashion, that such searches could raise suspicions of the subject individuals, may be time-consuming, and will not be available if the subject individuals do not travel internationally.

[9] During the subsequent wiretap that was authorized on September 28, 2017, agents did in fact conduct a border search on Nat's cellphone. The affidavit supporting the *next* reauthorization conceded this search was "helpful" but state that "*further* searches may raise . . . suspicion." Tremonte Decl., Ex. C, ¶ 76 (emphasis added).

Id.[10] This is the *only* statement of necessity as to Shikeba and Abdul, and it is plainly the kind of "generalized and conclusory statement[]" that the Second Circuit has held "will not satisfy Title III." *Concepcion*, 579 F.3d at 218. The wiretap application thus fails to meet the statutory requirement to establish that other investigative techniques have or will fail in order to justify the "greatest of all invasions of privacy" for Abdul and Shikeba, the real-time interception of their private communications. *Berger*, 388 U.S. at 58 (Douglas, J., concurring).[11]

C. The Szwalek Affidavit's Claims of Probable Cause and Necessity Were Based on Material Omissions

The fruits of the wiretap should also be suppressed, or, in the alternative, a *Franks* hearing should be ordered because the Szwalek Affidavit omitted significant information which, especially given the deficient allegations of necessity discussed above, would likely have caused the authorizing district judges to deny the government's application for the wiretap. Specifically, the Szwalek Affidavit—like the search warrant application—implied a connection between the Tronix Companies and the National Companies, but did not make clear that no such connection existed other than the family relationship between the principals and the fact of one common employee. Had the authorizing district judges understood that the allegations relating to Nat and

[10] As will be discussed further below, the paragraph omits to mention that Shikeba and Abdul both consented to the search of their phones at the border.

[11] The subsequent re-authorizations of the wiretap, which occurred on September 28, 2017, October 28, 2017, November 29, 2017, December 29, 2017, and January 28, 2018 contained no additional facts supporting necessity. The reauthorization requests did contain new facts learned from the prior interception of Shikeba's phone, which, for the reasons discussed above, should not have been authorized. But even so, the standard for authorization of a wiretap—whether as an initial matter or as a reauthorization—is not whether prior interceptions of the subject telephone have produced useful information; rather, it is whether the agent can show that "there is a genuine need" for a wiretap because of the deficiencies of other investigative techniques. *Dalia*, 441 U.S. at 250.

the Tronix employees simply had no bearing on whether a wiretap was appropriate as to Shikeba and Abdul, they would not have authorized it.

In addition, the wiretap application relied heavily on allegations concerning the CBP Regulatory Audit of ISK, alleging that Shikeba's concerns about the audit indicated a desire to conceal money laundering activity, rather than the common concern of any business-owner about being audited. But the Szwalek Affidavit failed to mention that ISK cooperated fully with the audit, voluntarily provided information to CBP, passed the audit with only a few areas that the agency identified as requiring improved bookkeeping, and undertook changes to implement the agency's recommendations. *See* Tremonte Decl. ¶ 9. Instead, the Affidavit indicated, misleadingly, in a footnote, that CBP had concluded the company was engaged in TBML. Had the authorizing judges been given the full picture of the audit, the allegations regarding it would have been largely discounted from their probable cause findings.

Finally, as noted above, the only specific allegation regarding the necessity requirement of Title III as to Shikeba and Abdul was the allegation concerning the *successful* border searches of their phones, and the assertion (without support) that further searches would raise suspicions. But the Szwalek Affidavit failed to inform the district judges that Shikeba and Abdul had *consented* to the searches of their phones at the border, consistent with their habit of disclosure to the government as evidenced during the CBP audit. *See* Tremonte Decl., ¶ 25. The inclusion of this material information would likely have altered the quantum of evidence going to the essential necessity component of the wiretap application.

These omissions of material information from the Szwalek Affidavit render the authorizations of the wiretap unworthy of deference. *See Rajaratnam I*, 2010 WL 4867402, at *7. The Court should suppress the fruits of the wiretap, or order a *Franks* hearing to determine

whether these omissions were made deliberately or in reckless disregard of the truth. *See Rajaratnam II*, 719 F.3d at 146.

D. The Government Failed in Its Minimization Duty

The agents who monitored the phones in this case did not minimize the interceptions properly. On many occasions, calls were intercepted for more than two minutes, despite the fact that the subject matter discussed in the calls had nothing whatever to do with the purported money laundering schemes described in the Szwalek Affidavits in support of the government's application for a wiretap. An "objective assessment of the monitoring officers' good-faith efforts to comply with the minimization requirement . . . of § 2518(5)" compels a finding that the government failed to minimize properly the calls it intercepted. *Scott*, 436 U.S. at 135-37; *see also Goffer*, 756 F. Supp. 2d at 595 (finding that law enforcement agents failed to minimize calls appropriately).

Examples of the monitoring officers' failure to minimize irrelevant intercepted calls, attached to the Tremonte Declaration as Exhibit N, include a discussion between Shikeba and her husband on September 15, 2017 about attending a bar-b-que at her sister-in-law's house[12], followed by a discussion about an employee of her husband's art gallery; an October 6, 2017 call from Shikeba to her parents letting them know that she and her husband are taking a trip to Virginia and explaining their childcare arrangements during the trip; a discussion on October 21, 2017 between Shikeba and Abdul about their elderly parents' plan to travel to Saudi Arabia for the annual pilgrimage to Mecca and which family members can make the trip to assist them. Other calls captured on the wiretap include a solicitation call to continue Shikeba's financial

[12] The line sheets provided in discovery incorrectly transcribe the sister-in-law's name as "Enayat," when it clearly can be heard as "Sonia."

support of Memorial Sloan Kettering Cancer Center and conversations about the goings-on at the mosque the family attends. These are just a few of many such interceptions.

The defendants recognize that courts are reluctant to suppress a wiretap in its entirety for a failure to properly minimize the conversations intercepted. *See, e.g.*, *Goffer*, 756 F. Supp.2d at 595. At a minimum, however, the Court should issue an order suppressing all intercepted calls of more than two minutes in length that concern topics other than transactions in cell phones or banking issues relating to the business of the National Companies. *See id.* at 595-96; *United States v. King*, 991 F. Supp. 77, 92 n.16 (E.D.N.Y. 1998); *United States v. Orena*, 883 F. Supp. 849, 855 (E.D.N.Y. 1995).

V. The Court Should Order a Bill of Particulars as to the Structuring Count and the Travel and Transportation in Aid of Racketeering Count

While the Indictment, search warrant and wiretap applications, and the government's "Highlights Presentation" to defendants, *see* Tremonte Decl. ¶ 23, have provided a commendable degree of pretrial disclosure in this case, on Count Five of the Indictment, the structuring count, the defendants still are unaware of which financial transactions the government alleges to be structured. And with respect to Count Six, the Travel and Transportation in Aid of Racketeering Count, the defendants do not know which trips the government contends were taken in furtherance of the crime charged in Count Six, the particular persons who failed to file the currency transaction reports referenced in Count Six; the occasions when said persons failed to file the currency transaction reports referenced in Count Six; and the particular user and use of the mails described generally in Count Six. The Court should order a bill of particulars on both Counts Five and Six.[13]

[13] Abdul demanded these particulars in his counsel's letter of December 4, 2018. Tremonte Decl., Ex. O.

Rule 7(f) of the Federal Rules of Criminal Procedure permits the Court to order a bill of particulars "to identify with sufficient particularity the nature of the charge . . . , thereby enabling [the] defendant[s] to prepare for trial, [and] to prevent surprise." *United States v. Bortnovsky*, 820 F.2d 572, 574 (2d Cir. 1987); *see* Fed. R. Crim. P. 7(f). A bill of particulars should be ordered "where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused." *United States v. Torres*, 901 F.2d 205, 234 (2d Cir. 1990). As to structuring, the Second Circuit has held that "(1) the defendant must, in fact, have engaged in acts of structuring; (2) he must have done so with knowledge that the financial institutions involved were legally obligated to report currency transactions in excess of $10,000; and (3) he must have acted with the intent to evade this reporting requirement" in order for the government to prove a charge of structuring. *United States v. MacPherson*, 424 F.3d 183, 189 (2d Cir. 2005).

The government has pointed to certain Whatsapp communications that show the uncontested fact of Shikeba's knowledge of the legal obligation to report deposits in excess of $10,000. But it has provided no information as to which deposits it considers to be structured nor any evidence of intent to evade the reporting requirements. Such intent may be proven by independent evidence of a defendant's state of mind or by a pattern of structured transactions. *See United States v. Taylor*, 816 F.3d 12, 23 (2d Cir. 2016). Here, the discovery does not provide independent evidence of an intent to evade the reporting requirements—indeed, the discovery is replete with bank records showing numerous cash deposits *above* $10,000 and the filing of IRS Forms 8300 by the National Companies reporting cash receipts from customers in excess of $10,000. *See id.* at 25 (evidence of structuring insufficient where "credit union's records showed that [defendant] made multiple single deposits exceeding $10,000 during the

same period in which [defendant] was supposedly structuring transactions to avoid CTR filings").[14] To provide the defendants with the notice and information they need to defend the structuring charge, the Court should order the government to provide a bill of particulars indicating which transactions it considers to be structured.

In addition, Count Six charges generally that the defendants traveled in interstate commerce and used the mails in furtherance of an alleged conspiracy to prevent banks from filing CTR forms and undefined money laundering. But Count Six does not charge which defendants traveled; or when they traveled; or where they traveled to, in furtherance of the undefined money laundering transactions alleged in Count Six. Nor does Count Six charge which items were mailed; who mailed them; when they were mailed; or to whom they were mailed in furtherance of the undefined money laundering transactions alleged in Count Six. Count Six does not specify any particular transactions–out of the thousands of transactions included in the bank accounts of Tronix and National during the lengthy period charged in the Indictment–as the subject of its allegation. Without knowing what transactions are at issue; which mailings or trips are at issue; and which defendants mailed, received mail or traveled in furtherance of the money laundering conspiracy referenced in Count Six, the defendants cannot possibly defend themselves against the general allegations of Count Six, which are untethered to any particular act or event. In these circumstances, the particulars demanded by Abdul in his December 4, 2018 letter, Tremonte Decl., Ex.O, are clearly appropriate and the Court should order the government to provide the particulars demanded.

---

[14] In a meeting on January 14, 2020, the government informed counsel for Shikeba that the alleged structured transactions occurred primarily in National's Habib Bank account and Devon Bank account (the latter of which was not listed in the Indictment). *See* Tremonte Decl. ¶ 24. We have reviewed the records of transactions in those accounts and remain uncertain of which transactions the government considers to be structured.

VI. The Court Should Order the Government to Produce Its Files Concerning the Internal Revenue Service's Audit of the National Companies Form 8300 Compliance

On December 10, 2018, Abdul demanded that the government produce its "reports" concerning any government audits of the National Companies during the period from 2013 to 2018. Tremonte Decl., Ex. P. Thereafter, on May 6, 2019, Abdul reiterated this demand, requesting the government's files concerning, *inter alia*, the audits of the National Companies' compliance with IRS Form 8300 requirements and other regulations. *See id.* The government thereafter produced records relating to the CBP examination of certain of the National Companies. Tremonte Decl., Ex. Q. However, to date, Defendants have not received any files concerning the IRS's audits of the National Companies' compliance with Form 8300 requirements.

As Abdul's counsel has previously explained, the National Companies' compliance with Form 8300 regulations will be reflected in the government's files and is therefore *Brady* material, to which Abdul and his co-defendants are entitled. To date, the government has not produced these items, which were requested by Abdul in December 2018 and May 2019. We respectfully request that the Court direct the government to produce its files and any other evidence in its possession concerning any examination or audit of the National Companies' compliance with the requirement to file IRS Form 8300.

VII. The Court Should Order That a Jury Questionnaire Be Used During Voir Dire

It is well established that a jury questionnaire may be an effective aide in the voir dire process, which the Court may require in its broad discretion to manage jury selection. *See Rosales-Lopez v. United States*, 451 U.S. 182, 188 (1981); *United States v. Salameh*, 152 F.3d 88, 121 (2d Cir. 1998). As the Second Circuit has noted, "District courts routinely employ

questionnaires to facilitate voir dire in a number of circumstances," and the "use of such a procedure as a preliminary screening tool falls well within the district court's broad discretion." *United States v. Quinones*, 511 F.3d 289, 299-300 (2d Cir. 2007). Written questionnaires are often used when a large number of prospective jurors are called in a case; where an anonymous jury is to be empaneled; where there has been extensive pre-trial publicity; or where the death penalty is sought. *Id.* However, the Court's discretion is not restricted such cases.

There are sound reasons to employ a written questionnaire in the voir dire process in this case. First, the defendants are members of a Muslim minority from Afghanistan. Their national origin and religion are facts that require careful scrutiny to ferret out bias in the jury pool. Prospective jurors who harbor such bias are unlikely to admit it in open court before their fellow jurors. Moreover, research has established the prevalence of *unconscious* or "implicit" bias across a range of decision-making processes. *See, e.g.*, Hoffman, K., *Racial bias in pain assessment and treatment recommendations, and false beliefs about biological differences between blacks and whites*, Proceedings of the National Academy of Sciences, Apr. 4, 2016; Pager, D., *Discrimination in Law-Wage Labor Market: A Field Experiment*, Am. Sociological Rev., Oct. 1, 2009. A written questionnaire, tailored to uncover jurors' private and implicit feelings about the defendants, will allow for more targeted follow-up voir dire on this issue and provide for a fair and impartial jury.

More generally, a written questionnaire will benefit all parties to this case by making jury selection quicker and smoother. As noted above, it is likely that multiple defendants will be on trial together in this case. If the Court employs a questionnaire, much of the basic information about the prospective jurors can be gleaned from them before the selection process begins. This will permit the defendants and the government to agree on a number of challenges for cause and

excuses for hardship before the voir dire process begins, winnowing down the venire panel and making the jury selection process with the remaining jurors more efficient. In addition, in a multi-defendant case, the defendants will be negotiating with each other and trying to agree on their limited number of peremptory challenges. Using a questionnaire will allow the defendants to begin the process of deciding which jurors they agree should be challenged with peremptory challenges if necessary. Having questionnaires in hand when voir dire begins will result in less negotiation in the courtroom as the voir dire proceeds, making the jury selection process smoother and quicker.

CONCLUSION

For the foregoing reasons, the Court should enter an order (1) dismissing (or severing) Counts One, Five, and Six of the Indictment as duplicitous; (2) severing the trials of the National Defendants and the Tronix Defendants; (3) suppressing the fruits of the search of Abdul and Shikeba's homes and of the office of National; (4) suppressing the fruits of the wiretap as to Abdul and Shikeba, or, in the alternative, ordering a *Franks* hearing; (5) ordering the government to provide a bill of particulars as to the structured financial transactions it intends to prove at trial and as to the travel in aid of racketeering count; (6) ordering the government to produce *Brady* material relating to the Form 8300 audit; and (7) ordering the use of a jury questionnaire during voir dire.

Dated: New York, New York
March 6, 2020

Respectfully submitted,

/s/Roland G. Riopelle
Roland G. Riopelle
SERCARZ & RIOPELLE, LLP
810 Seventh Ave., Suite 620
New York, NY 10019

Attorneys for Abdulrahman Khwaja

/s/Michael Tremonte
Michael Tremonte
Noam Biale
SHER TREMONTE LLP
90 Broad St., 23rd Floor
New York, NY 10004

Attorneys for Shikeba Rhamatzada